UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/675,262	09/28/2000	Jesse R. Walker	42390P9007	3019

8791 7590 03/18/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD, SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
CHO, UN C	

ART UNIT	PAPER NUMBER
2682	8

DATE MAILED: 03/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/675,262	WALKER, JESSE R.	
	Examiner	Art Unit	
	Un C Cho	2682	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Ala-Laurila et al. (US 6,587,680).

Regarding claim 1, Ala-Laurila teaches a method for establishing a secured roaming among mobile terminal, an old-AP (Fig. 2, 14) (Access Point) and a new-AP (Fig. 2, 114) (Access Point). Moreover, Ala-Laurila teaches that there already exists a security association between the mobile terminal and the current or old-AP (Ala-Laurila, Col. 8, lines 1 – 6). In other words, it is assumed that the first secured session has been established with the mobile terminal prior to a second ticket request. Ala-Laurila also teaches that the mobile terminal indicates to the current or old-AP that handover is required and when the message is received by the old-AP it retrieves security association parameters (SA) from its security association database and relaying a response message to the mobile terminal (Ala-Laurila, Col. 10, lines 39 – 57).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila in view of Norefors et al. (US 6,370,380).

Regarding claim 2, Ala-Laurila fails to teach applying the second ticket and a group identity shared by the first and the second access points to establish a second secured session between the wireless station and the second access point. However, Norefors teaches that applying in the message a hash code, which is a key that is shared only by the two access points to establish a secure handover between the mobile terminal and the second access point (AP_{NEW}) (Norefors, Col. 4, lines 13 – 38). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Norefors to Ala-Laurila in order to protect communications associated with a mobile terminal against unauthorized intrusion when the mobile terminal undergoes a handover from one access point to another.

5. Claims 3, 5 – 9 and 11 – 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila in view of Brown et al. (US 5,689,563).

Regarding claim 3, Ala-Laurila fails to teach that the authentication server dynamically generating a first and a second session keys to include in the first and the second tickets and the authentication server encrypting the first and the second tickets with a first and a second encryption keys. However, Brown teaches the authenticating unit generating a first and a second session keys to include in the first and the second tickets and the authenticating unit encrypting the first and the second tickets with a first and a second encryption keys (Brown, Col. 3, line 63 through Col. 4, line 8). Therefore, it would have been obvious to one of ordinary skill in the art the time the invention was made to provide the teaching of Brown to Ala-Laurila to create an encryption technique to alleviate problems associated with packetized data.

Regarding claim 5, Ala-Laurila fails to teach that the first access point appending application specific information to the second ticket to formulate a combined message and the first access point encrypting the combined message with the first session key. However, Brown teaches the first fixed network communication unit 130 appending application specific information to the second ticket to formulate a combined message and the first fixed network communication unit encrypting the combined message with the first session key (Brown, Col. 6, lines 35 – 54). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Brown to Ala-Laurila to create an encryption technique to alleviate problems associated with packetized data.

Regarding claim 6, Ala-Laurila fails to teach that the application specific information further comprises the first access point's selected time and random number. However, Brown teaches the application specific information further comprises the first fixed network communication unit 130 selected instant specific information and random challenge (RAND) (Brown, Col. 6, lines 14 – 21 and Col. 7, lines 39 – 48). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Brown to Ala-Laurila to create an encryption technique to alleviate problems associated with packetized data.

Regarding claim 7, Ala-Laurila teaches that there already exists a security association between the mobile terminal and the current or old-AP (Ala-Laurila, Col. 8, lines 1 – 6). In other words, it is assumed that the first secured session has been established with the mobile terminal prior to a second ticket request. Ala-Laurila also teaches that the mobile terminal indicates to the current or old-AP that handover is required and when the message is received by the old-AP it retrieves security association parameters (SA) from its security association database and relaying a response message to the mobile terminal (Ala-Laurila, Col. 10, lines 39 – 57). Ala-Laurila also teaches that the control element (Fig. 1, 28) comprises a comparator (Fig. 1, 32), which includes security functions (Ala-Laurila, Col. 7, lines 14 – 30). However, Ala-Laurila fails to teach that an access point is comprised of an antenna, a filter coupled to the antenna, a receiver and a transmitter coupled to the filter and a control unit coupled to the receiver and the

transmitter and coupled to a wired-network connection interface. In contrast, Brown teaches an antenna (Fig. 1, 154), inherently a filter coupled to the antenna, a receiver and a transmitter (Fig. 1, 152) coupled to the filter and a switch center (Fig. 1, 128) coupled to the receiver and the transmitter and coupled to a wired-network connection interface (Fig. 1, 132) wherein the switch center comprises a database (Fig. 1, 136). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Brown to Ala-Laurila to create an encryption technique to alleviate problems associated with packetized data.

Regarding claim 8, Ala-Laurila teaches the control element (Fig. 1, 28) forwarding the second ticket request. However, Ala-Laurila fails to teach that the control unit comprises an encryption/decryption engine to decrypt the second ticket request before the authentication protocol engine forwards the second ticket request. In contrast, Brown teaches that a switch center (Fig. 1, 128) decrypting the second ticket request (Brown, Col. 8, lines 16 – 24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Brown to Ala-Laurila to create an encryption technique to alleviate problems associated with packetized data.

Regarding claim 9, the claim is interpreted and rejected for the same reason as set forth in claim 3.

Regarding claim 11, Ala-Laurila fails to teach that the access point further comprises the authentication protocol engine to append application specific

information to the second ticket to formulate a combined message and the encryption/decryption engine to encrypt the combined message with the first session key. However, Brown teaches that the first fixed network communication unit (Fig. 1, 130) appends application specific information to the second ticket to formulate a combined message with the first session key (Brown, Col. 6, lines 35 – 64). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Brown to Ala-Laurila to create an encryption technique to alleviate problems associated with packetized data.

Regarding claim 12, the claim is interpreted and rejected for the same reason as set forth in claim 6.

Regarding claim 13, Ala-Laurila teaches a control element (Fig. 1, 28) comprising a comparator (Fig. 1, 32), which includes security functions that requests a handover and old-AP retrieves security association parameters from its security association data base after having established a first secured session with the old-AP (Ala-Laurila, Col. 8, lines 1 – 6 and Col. 10, lines 39 – 57). However, Ala-Laurila fails to teach a wireless station comprising an antenna, a filter coupled to the antenna, a receiver and a transmitter coupled to the filter, and a control unit coupled to the receiver and the transmitter. In contrast, Brown teaches an antenna (Fig. 1, 124), inherently a filter coupled to the antenna, a subscriber unit (Fig. 1, 122), a receiver and a transmitter (Fig. 1, 122) coupled to the filter and a micro processing stage (Fig. 1, 118) coupled to the receiver and

the transmitter wherein the micro processing stage is also coupled to the encryptor/decryptor. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Brown to Ala-Laurila to create an encryption technique to alleviate problems associated with packetized data.

6. Claims 4 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila in view of Brown as applied to claim 3 above, and further in view of Hauser et al. (US 5,778,065).

Regarding claim 4, Ala-Laurila as modified by Brown fails to teach that the first and second session keys have limited lifetime. However, Hauser teaches that session keys have limited lifetime (Hauser, Col. 1, lines 9 – 17). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Hauser to Ala-Laurila to Brown to provide a secure and compact authentication protocol between a user and the authentication server without sacrificing any of the important advantages of the known systems.

Regarding claim 10, the claim is interpreted and rejected for the same reason as set forth in claim 4.

7. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ala-Laurila in view of Brown as applied to claim 13 above and further in view of Norefors et al. (US 6,370,380).

Regarding claim 14, Ala-Laurila as modified by Brown fails to teach that the authentication protocol engine applies the second ticket and a group identity shared by the first and the second access points to establish a second secured session between the wireless station and the second access point. However, Norefors teaches that the mobile terminal re-encrypts the security token using an encryption key that it shares with the second access point then applying in the message a hash code, which is a key that is shared only by the two access points to establish a secure handover between the mobile terminal and the second access point (AP_{NEW}) (Norefors, Col. 2, lines 17 – 34 and Col. 4, lines 13 – 38). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Norefors to Ala-Laurila in order to protect communications associated with a mobile terminal against unauthorized intrusion when the mobile terminal undergoes a handover from one access point to another.

8. Claims 15, 17, 18, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over admitted prior art in view of Ala-Laurila and Brown.

Regarding claim 15, the admitted prior art (Figure 1) teaches a wireless roaming system comprising a wired medium (Fig. 1, 112), a wireless medium

(Fig. 1, 106), a server (Fig. 1, 114) coupled to the wired medium and a wireless station (Fig. 1, 108) coupled to the wireless medium, and an access point (Fig. 1, 100) coupled to the wireless medium and the wired medium. However, the admitted prior art fails to teach a first control unit, comprising a first authentication protocol engine to request a first ticket from the authentication server and use the first ticket to establish a first secured session with the wireless station and in response to a second ticket request from the wireless station through the first secured session, to forward the second ticket request to the authentication server and relays a resulting second ticket form the authentication server to the wireless station. In contrast, Brown teaches a fixed network communication unit (Fig. 1, 130) comprising a switching center (Fig. 1, 128), having a encryptor/decryptor (Fig. 1, 150). Moreover, Ala-Laurila teaches that there already exists a security association between the mobile terminal and the current or old-AP (Ala-Laurila, Col. 8, lines 1 – 6). In other words, it is assumed that the first secured session has been established with the mobile terminal prior to a second ticket request. Ala-Laurila also teaches that the mobile terminal indicates to the current or old-AP that handover is required and when the message is received by the old-AP it retrieves security association parameters (SA) from its security association database and relaying a response message to the mobile terminal (Ala-Laurila, Col. 10, lines 39 – 57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Brown and Ala-Laurila to the admitted prior art to provide an efficient

method/apparatus for re-establishing an existing security association when a handover event occurs in a radio communications system.

Regarding claim 17, admitted prior art as modified by Ala-Laurila and Brown teaches a switch center (Brown, Fig. 1, 128) comprising an encryptor/decryptor to decrypt the second ticket request (Brown, Col. 8, lines 16 – 24). Moreover, Ala-Laurila teaches forwarding the second ticket request (Ala-Laurila, Col. 10, lines 39 – 57).

Regarding claim 18, the admitted prior art fails to teach the authentication server dynamically generating a first and a second session keys to include in the first and the second tickets and encrypting the first and the second tickets with a first and a second encryption keys. However, Brown teaches the authenticating unit generating a first and a second session keys to include in the first and the second tickets and the authenticating unit encrypting the first and the second tickets with a first and a second encryption keys (Brown, Col. 3, line 63 through Col. 4, line 8). Therefore, it would have been obvious to one of ordinary skill in the art the time the invention was made to provide the teaching of Brown to Ala-Laurila to create an encryption technique to alleviate problems associated with packetized data.

Regarding claim 20, the admitted prior art as modified by Ala-Laurila fails to teach that the first authentication protocol engine to append application specific information to the second ticket to formulate a combined message and the first access point encrypting the combined message with the first session

key. However, Brown teaches the first fixed network communication unit 130 appending application specific information to the second ticket to formulate a combined message and the first fixed network communication unit encrypting the combined message with the first session key (Brown, Col. 6, lines 35 – 54). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Brown to Ala-Laurila to create an encryption technique to alleviate problems associated with packetized data.

Regarding claim 21, the admitted prior art as modified by Ala-Laurila fails to teach that the application specific information further comprises the access point's selected time and random number. However, Brown teaches the application specific information further comprises the first fixed network communication unit 130 selected instant specific information and random challenge (RAND) (Brown, Col. 6, lines 14 – 21 and Col. 7, lines 39 – 48). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Brown to Ala-Laurila to create an encryption technique to alleviate problems associated with packetized data.

9. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over the admitted prior art in view of Ala-Laurila and Brown as applied to claim 15 above, and further in view of Norefors et al. (US 6,370,380).

Regarding claim 16, the admitted prior art as modified by Ala-Laurila and Brown fails to teach that the authentication protocol engine applies the second ticket and a group identity shared by the first and the second access points to establish a second secured session between the wireless station and the second access point. However, Norefors teaches that the mobile terminal re-encrypts the security token using an encryption key that it shares with the second access point then applying in the message a hash code, which is a key that is shared only by the two access points to establish a secure handover between the mobile terminal and the second access point (AP_{NEW}) (Norefors, Col. 2, lines 17 – 34 and Col. 4, lines 13 – 38). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the teaching of Norefors to Ala-Laurila in order to protect communications associated with a mobile terminal against unauthorized intrusion when the mobile terminal undergoes a handover from one access point to another.

10. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over admitted prior art in view of Ala-Laurila and Brown as applied to claim 15 above, and further in view of Hauser et al. (US 5,778,065).

Regarding claim 19, the admitted prior art as modified by Ala-Laurila and Brown fails to teach that the first and second session keys have limited lifetime. However, Hauser teaches that session keys have limited lifetime (Hauser, Col. 1, lines 9 – 17). Therefore, it would have been obvious to one of ordinary skill in the

art at the time the invention was made to provide the teaching of Hauser to Ala-Laurila to Brown to provide a secure and compact authentication protocol between a user and the authentication server without sacrificing any of the important advantages of the known systems.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Un C Cho whose telephone number is (703)305-8725. The examiner can normally be reached on M ~ F 8:00AM to 4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Vivian Chin can be reached on (703)308-6739. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LEE NGUYEN
PRIMARY EXAMINER

Un C Cho UC
Examiner
Art Unit 2682
3/10/2004